

NATIONAL MARINE FISHERIES SERVICE INSTRUCTION 32-106-01
December 15, 2014

Information Management
HEADQUARTERS NETWORK SERVER DEPLOYMENT POLICY

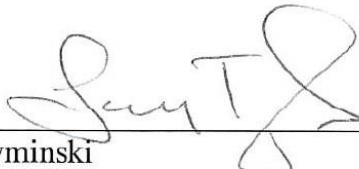
SERVER DEPLOYMENT PROCEDURES

NOTICE: This publication is available at: <http://www.nmfs.noaa.gov/op/pds/>

OPR: F/CIO
Type of Issuance: Initial

Certified by: F/CIO (L. Tyminski)

SUMMARY OF REVISIONS:

Signed  DEC 1 2014
Larry Tyminski _____
NMFS Chief Information Officer Date

Overview/Background

The NOAA Fisheries Office of the Chief Information Officer (OCIO) is responsible for deploying IT systems which serve Fisheries Headquarters at many levels. These systems provide services for employees at different levels in Fisheries program offices in the organization. In order to deploy these systems NMFS Office of the CIO must consider multiple factors to ensure safe and successful IT system lifecycles.

Financial and human resources availability is an extremely critical factor that should be considered when evaluating the need for a new system. Office of the CIO must ensure that financial and human resources are available to maintain the system after its initial deployment.

In addition to these resources, Office of the CIO must also address many computer related threats. These threats include external probes, computer viruses and denial of service attacks to name a few. These activities represent a significant risk to the agency's reputation and to its mission. These threats demand that our systems be deployed with industry best practices and protections.

Coordination between the Office of the CIO, headquarters program offices and third-party solution providers not only ensure that the system being deployed meet the customer's needs, but also ensures that the system selected meet the DOC, NOAA, security and other high level requirements.

Goals & Objectives

The purpose of this document is to outline the process of deploying IT systems in the Fisheries HQ Office of the Chief Information Officer. This process will be used to provide a consistent and repeatable process for reviewing; funding, designing and deploying Fisheries headquarter IT systems. The information included in this document excludes the deployment of personal computers used by a single employee performing routine administrative function, such as word processing and electronic messaging.

Fisheries Office of the Chief Information Officer is responsible for purchasing and maintaining server hardware, primarily located in the Fisheries headquarters data center. The data center's rack space, power, and cooling capacities are quickly being consumed, and the strategic environmental goals for organization, aimed at reducing the datacenter's carbon footprint, require the more efficient use of computing resources. Additionally, in order to sustain and improve its server management numbers, IT Services needs to be able to support a variety of hardware platforms in an efficient manner.

Implementation Guidelines

The Office Information Technology Coordinator (OITC) of Fisheries Program Offices wishing to deploy new server hardware at Fisheries Headquarters, regardless of Operating System, will submit a request to the Headquarters Infrastructure Team Leader, following are general guidelines:

- Purpose of the server deployment
- The OITC and his/her manager define the lifecycle and budget for the system
- The application sponsor meets with the Office of the CIO to review the projects' technical requirements and discuss available budget.
- The application sponsor and Office of the CIO enter a temporary agreement to evaluate and propose a solution
- The program office appoint an application owner and sponsor
- The application sponsor and Office of the CIO coordinate to create a final set of requirements (*Storage and server requirements, service level agreement, etc.*)
- The application owner, sponsor and Office of the CIO coordinate to develop a service level agreement for the proposed system (*Expected Uptime, Recovery Time objective, Recovery Point Objective, etc.*)
- The Office of the CIO provides a cost estimate to deploy and maintain the system requirements over the specified lifecycle.
- The sponsor coordinates with his/her supervisor to ensure that the office has adequate funding to support the system through its lifecycle.
- The application owner, third-party-software-engineer and Office of the CIO coordinate to develop a system architecture, security model and operational best practices for the system
- The Office of the CIO and originating office managers enter an official (documented) Service Level Agreement (expected life-cycle, cost, end-of-contract, etc.)
- The application owner, sponsor and Office of the CIO create a change request to deploy the system
- The change control board will elevate this request as necessary to ensure that it is aligned with the IT process and procedures (*NMFS policies, IT security, etc.*)
- Deployment of any production level system requires an approved "System Change Request"
- The System Change Request (SCR) must include (all pertinent documentation):
 - a. Description of the system
 - b. Roles and responsibilities (app owner, sponsors, technical staff, etc.)
 - c. Architectural Diagram
 - d. Summary of security and operational service level agreement
 - e. Technical Details for implementation
- The approved SCR is then processed by a system administrator to ensure that all best

practices and operational procedures are implemented

- Modifications to the system are requested and tracked by the OCIO Change Control Board

Evaluation Criteria

Office of the CIO established the following guidelines for deploying new network servers in HQ datacenter:

- Greater density of physical servers in a data center.
- Reduced power consumption per equivalent number of stand-alone servers.
- Easier and quicker physical server deployment.
- Lower overall provisioning and associated monthly rates for program offices.
- No additional hardware for console management.
- Power, console, and network cabling are simplified and reduced.

Success in this area is really a sub-component of success in other areas: reductions in power consumption and space per server, and servers-per-sys admin.

References

- National Institute of Standards and Technology (NIST) SP 800-30, *Risk Assessment Guide for Information Technology Systems*.
- National Institute of Standards and Technology (NIST) SP 800-123, *Guide to General Server Security, July 2008*.
- IT Security - All NOAA system will be compliant with the Federal Information Security Management Act (FISMA) and NOAA's IT Security Architecture, Policies, and Procedures.